SOFTWARE USING METHOD AND SOFTWARE DISTRIBUTION SYSTEM

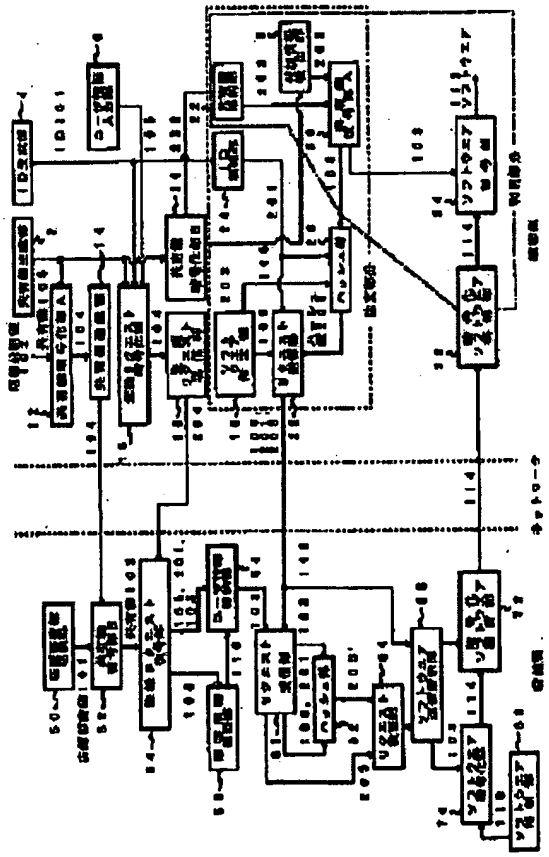
Patent number:	JP9244886
Publication date:	1997-09-19
Inventor:	TAKAHASHI TOSHINARI; NOGAMI HIROYASU
Applicant:	TOKYO SHIBAURA ELECTRIC CO
Classification:	
- International:	G06F9/06
- european:	G06F1/00N7R2; G06F21/00N7D
Application number:	JP19960053407 19960311
Priority number(s):	JP19960053407 19960311

Also published as:

E P0795809 (A2)
US 6195432 (B1)
E P0795809 (A3)

Abstract of **JP9244886**

PROBLEM TO BE SOLVED: To prevent software from illegally being copied by deciphering specific ciphered software provided by a provider at a request to provide the software by using a stored specific common key. SOLUTION: A customer ciphers a common key 103 generated by a common key generation part 2 through a ciphering part 12 by utilizing a store open key 102, and a common key deciphering part 52 on a store side deciphers the received ciphered common key by using a store secret key 101 to obtain a common key 103. Then when a request transmission part 26 sends article specification data, an ID, etc., to the store side, a software transmission indication part 66 sends the common key 103 to a software deciphering part 70 and also instructs a ciphered software transmission part 72 to send software. A deciphering part 70 deciphers the corresponding software read out of a software storage part 68 with the common key 103 and sends it; and the software is stored in a ciphered software storage part 32 on the customer side and a software deciphering part 34 takes the software out and deciphers it with the common key.



US. 6,195,432

(19)日本国特許庁（JP）　(12)公開特許公報(A)　(11)特許出願公開番号

特開平9－244886

(43)公開日　平成9年(1997)9月19日

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI	技術表示箇所
G06F 9/06	550		G06F 9/06	550E

審査請求　未請求　請求項の数7　OL　（全 13 頁）

(21)出願番号　特願平8－53407

(22)出願日　平成8年(1996)3月11日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　高橋　俊成
神奈川県川崎市幸区小向東芝町1番地　株式会社東芝研究開発センター内

(72)発明者　野上　宏康
神奈川県川崎市幸区小向東芝町1番地　株式会社東芝研究開発センター内

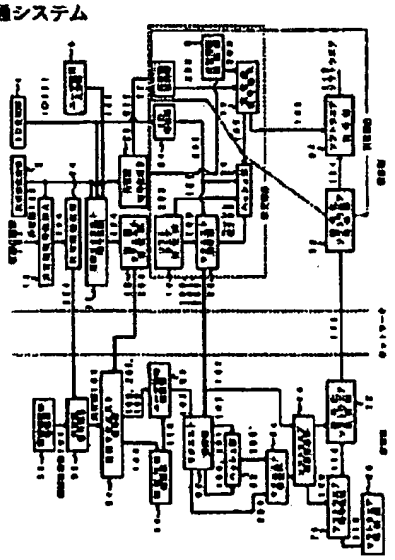
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　ソフトウエア利用方法及びソフトウエア流通システム

(57)【要約】

【課題】　利用者が簡易な操 作でネットワークを通じてソフトウエアを購入でき、ソフトウエア流通が公正な価格で安全に行われることを可能とし、ソフトウエアの違法コピーが困難なソフトウエア利用方法を提供すること。

【解決手段】　ソフトウェア利用者のソフトウェア料金の決済に関わる識別情報との対応付けが保証され、ソフトウェア提供者と利用者とで共有された共有鍵を記憶し、指定するソフトウエアの提供を前記ソフトウェア提供者に対して要求し、記憶された前記共有鍵を用いて、提供者より提供された指定の暗号化ソフトウェアを復号することを特徴とする。



【特許請求の範囲】
【請求項 1】ソフトウェア利用者のソフトウェア料金の決済に関わる識別情報との対応付けが保証され、ソフトウェア提供者と利用者とで共有された共有鍵を記憶し、指定するソフトウエアの提供を前記ソフトウェア提供者に対して要求し、
記憶された前記共有鍵を用いて、提供者より提供された指定の暗号化ソフトウェアを復号することを特徴とするソフトウェア利用方法。
【請求項 2】前記識別情報と前記共有鍵との対応付けの保証は、前記利用者が、前記共有鍵を生成し、この共有鍵を前記ソフトウェア提供者の持つ秘密鍵に対応する公開鍵を用いて暗号化して前記ソフトウェア提供者に与え、この共有鍵を用いて前記識別情報を暗号化して前記ソフトウェア提供者に与えることによりなされるものであ ることを特徴とする請求項 1に記載のソフトウェア利用方法。
【請求項 3】前記識別情報と前記共有鍵との対応付けの保証は、前記利用者が、前記共有鍵を生成し、この共有鍵および前記識別情報を前記ソフトウェア提供者の持つ秘密鍵に対応する公開鍵を用いて暗号化して前記ソフトウェア提供者に与えることによりなされるものであ ることを特徴とする請求項 1に記載のソフトウェア利用方法。
【請求項 4】共有鍵を記憶するにあ たっては、ソフトウエア利用に関する付加情報を検出し、検出した付加情報を用いて共有鍵を暗号化し、生成された暗号化共有鍵を記憶し、
暗号化ソフトウェアを復号するにあ たっては、ソフトウエア利用に関する付加情報を検出し、検出した付加情報を用いて暗号化共有鍵を復号し、取り出された共有鍵を用いて暗号化ソフトウェアを復号することを特徴とする請求項 1に記載のソフトウェア利用方法。
【請求項 5】復号により得られたソフトウェアを用いて、既に存在する他のソフトウェアを実行することを特徴とする請求項 1に記載のソフトウェア利用方法。
【請求項 6】ソフトウエア提供者が指定されたソフトウェアを暗号化して利用者に提供するソフトウエア流通システム において、
ソフトウェア料金の決済に関わる識別情報との対応付けが保証された共有鍵を記憶する、ソフトウェア提供者及び利用者側の双方に設けられた共有鍵記憶手段と、
指定するソフトウエアの提供の要求をソフトウエア提供者に送る、利用者側に設けられた要求送信手段と、
指定されたソフトウエアを前記共有鍵と関連付けて暗号化する、ソフトウエア提供者側に設けられたソフトウエア暗号化手段と、
この暗号化されたソフトウエアを前記利用者に送信する、ソフトウエア提供者側に設けられた暗号化ソフトウエア送信手段と、
受信した暗号化ソフトウエアを前記共有鍵と関連付けて復号する、利用者側に設けられたソフトウエア復号手段とを具備したことを特徴とするソフトウエア流通システム 。
【請求項 7】前記ソフトウエア提供者側に、
受信したソフトウエアの提供の要求が正当であ るか否かを前記共有鍵と関連付けて検査する要求検査手段と、
前記検査の結果、正当であ ると判断された場合にのみ、前記ソフトウエア暗号化手段と前記暗号化ソフトウエア送信手段に夫々暗号化と送信の実行を指示するソフトウエア送信指示手段とをさらに設けたことを特徴とする請求項 6に記載のソフトウエア流通システム 。

【発明の詳細な説明】
【０００１】
【発明の属する技術の分野】本発明は、ソフトウエア利用方法及びソフトウエア流通システム に関する。
【０００２】
【従来の技術】計算機および計算機ネットワークが普及し、ソフトウエアの流通は現金などを用いた従来の取引形態によらずとも、全て電子的に行うことができるようになった。
【０００３】ソフトウエアの流通に必要な最大の要求は、比較的容易にコピー（複写）を作成することのできるソフトウエアを流通させる際に、いかにしてソフトウエアを入手しようとする人が誰であ るかを特定し、安全に課金を行うかということであ る。
【０００４】従来、計算機ネットワーク上での課金のメカニズム は、暗号技術に基いた認証技術が用いられてきた。例えば、計算機ネットワークを使ってクレジットカード番号を伝える場合、通信回線を盗聴することによって他人がクレジットカード番号を盗めるのでは困るから、クレジットカード番号を暗号化しなければならなかった。
【０００５】一方、違法コピー防止の方法も考えられてきた。最も良く使われる方法は、ソフトウエアに何らかの暗号化を施し、データを復号する鍵（暗号鍵やパスワードなど）を持っている人だけが内容を知ることができる方法であ る。しかし、この方法によっても、パスワード自体を違法にコピーすることによって、ソフトウエアの違法コピーが可能となってしまう。
【０００６】これらの問題点をソフトウエアだけで完全に解決するのは困難であ ったことから、特殊なハードウエアを仮定した「超流通」と呼ばれるシステム が知られている。これは、あ るハードウエアの中身は所有者自身も解析することが不可能で、あ るデータを入力すると対応する何らかのデータを出力するというブラックボックスを使うものであ る。例えば、このブラックボックスの機能がなければ暗号が解けないという工夫は、公開鍵暗号方式など従来の暗号技術で実現することができる。しかし、この方式では、全ての顧客が自分専用のハードウ

エアを所持し、常にそのハードウエアを利用することが必要であるため現実的ではなく、また、仮にこのシステムを利用したとしても違法コピーを完全に防ぐことができるというわけではない。例えば、音楽を再生することがその人にしかできないとしても、その音楽を別の装置で録音してコピーすることはできる。このような制約から、「流通」システムは産業上、普及していない。

【０００７】図５は、暗号技術を応用して、クレジットカード番号をネットワーク上で安全に送るための従来技術を説明するための図である。図５で左側はソフトウエアを販売しようとする店舗側、右側は購入しようとする顧客側を示す。また、それらの間は両者を結ぶ電話回線やインターネットなどの計算機ネットワーク（以下これらをネットワークと略す）を示す。なお、店舗側の機能も顧客側の機能も基本的にはソフトウェアにより実現されるものである。

【０００８】店舗はあらかじめ公開鍵暗号方式による店舗秘密鍵１０１と店舗公開鍵１０２を持っている。店舗秘密鍵１０１は店舗秘密鍵格納部３５０に保存されており、他からはその内容を参照できない。店舗公開鍵１０２は公開されていて、誰でもネットワーク等を介して入手することができる。

【０００９】顧客がソフトウエアを購入する際には、まず店舗との安全な通信を確保するために共有鍵生成部３０２によって共有鍵１０３を生成する。これは他からは推測できない乱数を生成するものであり、共有鍵は、そのセッションに関して共有されることからセッション鍵とも呼ばれる。生成された共有鍵１０３は共有鍵暗号化部３１２によって、暗号化される。暗号化の際には店舗公開鍵１０２を利用する。

【００１０】共有鍵暗号化部３１２は生成した暗号化共有鍵１０４を共有鍵送信部３１４に送り、共有鍵送信部３１４はこれをネットワークを介して店舗側に送信する。店舗側の共有鍵復号部３５２は、受信した暗号化共有鍵１０４を店舗秘密鍵１０１を用いて復号し共有鍵１０３を得る。

【００１１】一方、情報暗号化部３１６は、共有鍵１０３を用いて任意の情報を暗号化する。例えば、クレジットカード番号を暗号化送信するために用いられる。情報暗号化部３１６で暗号化された暗号化情報１０７は、情報送信部３１８によってネットワークを介して店舗側に送信される。店舗側の情報復号部３５４は、受信した暗号化情報１０７を共有鍵１０３で復号し、顧客側から送られて来た情報を得る。

【００１２】このような手順により、クレジットカードなどの情報をネットワークを介して安全に送信することができる。なぜなら、店舗公開鍵１０２で暗号化された共有鍵１０３は、公開鍵暗号方式の性質により店舗秘密鍵１０１を所持する者しか復号することはできない。また、送られた情報は、この方法で共有鍵１０３を共有した店舗と顧客しか復号することはできないからである。

【００１３】以上の方法によって、実際にクレジットカード番号等を伝えた正規のユーザにのみソフトウエアを販売することができる。しかし、ソフトウエアは通常容易にコピーできるため、購入したソフトウェアをコピーして配布したり販売したりする違法行為に対する抑止は困難である。

【００１４】これを防ぐ方法として、ソフトウェアをそのまま販売するのではなく、特定のパスワードを入力しないと動作しないようにし、あるいは実行のたびに特定のサーバからライセンスを受けて実行させるなどといったさまざまな工夫がなされているが、決め手には欠ける。なぜなら、いかなる細工をしようとも、購入したソフトウェアを違法コピーするには、そのソフトウェアだけでなく、ソフトウェアの利用に必要な顧客側システム（ソフトウェア）の周辺部分の全てをコピーすれば、同一の利用環境を再現することができ、結局、コピーが可能であるからであり、リスクを負わずに違法コピー行為ができてしまう。

【００１５】一方、購入のたびにクレジットカード番号またはその顧客に与えられたユーザＩＤやパスワードをタイプするような煩雑な手続が必要なシステムである場合、例えば明日の天気予報に３円取る、といった粒度の細い課金は不可能であり（手続が煩雑であると価値の低いサービスは利用されなくなるため）、結果的に料金の高いソフトウエアしか流通せず、一部の権 利者は法外な利益を得、一部の権 利者は全く利益が上げられないという状態に陥り、ソフトウエアの流通が阻害される。これを防ぐために、例えば、クレジットカード番号を計算機に保存し、自動送信するようなメカニズム を用いても、その計算機が盗難にあえば、他人に不正利用されるおそれがあり、便利さと安全性を両立させることができない。

【００１６】

【発明が解決しようとする課題】上述したように、従来のソフトウエア流通システム では、クレジットカード番号などを盗まれずに電子的な購入依頼をすることはできるものの、購入したソフトウエアの違法コピーに対しては十分な配慮がなされていなかった。なぜなら、ソフトウエアの注文部分と利用部分とが顧客側から見て分離しているためであり、一旦ソフトウエアを購入してしまえば違法コピーを実現するためのさまざまな方法を施すことが可能だからである。

【００１７】また、従来方式によっては、例えば同じ顧客が別の計算機で同じソフトウエア（計算機プログラム）を利用する場合に再度料金を取るというような細かな課金方式を設定することが困難であった。

【００１８】本発明は、上記事情を考慮してなされたものであり、ソフトウエアの違法コピーを困難にしたソフトウエア利用方法及びソフトウエア流通システム を提供

することを目的とする。また、本発明は、利用者が簡易な操 作でネットワークを通じてソフトウエアを購入できるソフトウエア利用方法及びソフトウエア流通システムを提供することを目的とする。また、本発明は、ソフトウエア流通が公正な価格で安全に行われることを可能とするソフトウエア利用方法及びソフトウエア流通システム を提供することを目的とする。

【００１９】

【課題を解決するための手段】本発明に係るソフトウェア利用方法は、ソフトウェア利用者のソフトウェア料金の決済に関わる識別情報との対応付けが保証され、ソフトウェア提供者と利用者とで共有された共有鍵を記憶し、指定するソフトウエアの提供を前記ソフトウェア提供者に対して要求し、記憶された前記共有鍵を用いて、提供者より提供された指定の暗号化ソフトウェアを復号することを特徴とする。

【００２０】ここで、ソフトウエアとは、計算機プログラム 、データベース、情報検索サービスによって得られた結果、書籍、音楽、映画、テレビ放送、対戦型ゲームや電話あ るいは対話型テレビなどでインタラクティブに交換される情報など、物流を伴わずに電子的に送信することが可能なもの全てを含むものとする。

【００２１】ソフトウェア料金の決済に関わる識別情報とは、例えば、クレジットカード番号やその有効期限、暗証番号、あ るいは銀行の口座番号、特定の企業等から発行された決済に関わる会員番号等（例えばパソコン通信のユーザｉＤ）などであ る。

【００２２】本発明によれば、利用者は購入の際にクレジット・カード番号等のソフトウェア料金の決済に関わる識別情報を入力する必要がなく、手間をかけずに簡便な操 作でソフトウエアを購入することができる。このため、利用者は、クレジット・カード等（カードそのもの）を安全な場所に保管したままで、ソフトウエアの購入ができるので安全であ るという利点もあ る。

【００２３】また、ソフトウェア提供者は販売の際に利用者から上記識別情報を送信してもらわなくても、ソフトウエア流通に伴う課金等の認証を容易に行うことができる（安全に課金等を行うことができる）。

【００２４】以上によって、何に対して課金をするかといった細かな指定が可能であ ることと相まって、各ソフトウエアの価値に応じた適正な価格での販売が促進される。また、本発明によれば、共有鍵はソフトウエアの実行に対する鍵であ ると同時にソフトウエア購入の鍵でもあ るので、ソフトウエアの違法コピーを行うことが困難でリスクの高いものになる。従って、違法コピーは利用者にとっては不利益となり、違法行為を行う価値がなくなるので、購入したソフトウエアの再販売などの違法行為を防止することができる。

【００２５】さらに、利用者は、汎用用途のクレジット・カード等を使って、自発的に自分の希望するソフトウェア提供者からの購入を可能とする共有鍵を作成することができる。万一、共有鍵が盗まれても、用途が限定されているため、被害は少ない。

【００２６】好ましくは、前記識別情報と前記共有鍵との対応付けの保証は、前記利用者が、前記共有鍵を生成し、この共有鍵を前記ソフトウェア提供者の持つ秘密鍵に対応する公開鍵を用いて暗号化して前記ソフトウェア提供者に与え、この共有鍵を用いて前記識別情報を暗号化して前記ソフトウェア提供者に与えることによりなされるものであ ることを特徴とする。

【００２７】好ましくは、前記識別情報と前記共有鍵との対応付けの保証は、前記利用者が、前記共有鍵を生成し、この共有鍵および前記識別情報を前記ソフトウェア提供者の持つ秘密鍵に対応する公開鍵を用いて暗号化して前記ソフトウェア提供者に与えることによりなされるものであ ることを特徴とする。

【００２８】好ましくは、共有鍵を記憶するにあ たっては、ソフトウエア利用に関する付加情報を検出し、検出した付加情報を用いて共有鍵を暗号化し、生成された暗号化共有鍵を記憶し、暗号化ソフトウェアを復号するにあ たっては、ソフトウエア利用に関する付加情報を検出し、検出した付加情報を用いて暗号化共有鍵を復号し、取り出された共有鍵を用いて暗号化ソフトウェアを復号することを特徴とする。

【００２９】付加情報とは、例えばソフトウエア利用における付加的な条件やソフトウエア利用環境の情報であり、具体例としては、顧客の持つ計算機に固有の番号（ｈｏｓｔＩＤ）、利用しているＯＳの商品番号、そのユーザしか知り得ないパスワード、ユーザの持っているＩＣカードに入っているデータまたはＩＣカードに何らかのデータを与えて出力される結果データ、計算機に内蔵 された時計の時刻などが考えられる。

【００３０】これによって、例えば、暗号化共有鍵が盗難されても、他の計算機では正しい共有鍵が得られず、暗号化ソフトウェアを復号することができないので、盗難などによる安全性の低下を防止することができる。

【００３１】また、付加情報の内容を選択するかによって、さまざまな形態での課金方法が可能になる。例えば、同一のマシンであ ればずっとソフトウエアを使い続けられる、同一のマシンであ っても新しいＯＳになったときには再度料金を支払わなければソフトウエアが利用できなくなる、あ る時刻（日付）になったら再度お金を払う必要があ る、夜間の使用は無料であ る昼間の使用は制限されるなどといったことが可能となる。

【００３２】好ましくは、復号により得られたソフトウェアを用いて、既に存在する他のソフトウェアを実行することを特徴とする。例えば、有償の暗号化ソフトウエア（これを復号したものが、復号により得られたソフトウェアに相当する）を復号して得たソフトウエアがないと機能しない部分を含むソフトウエアを無償で配布して

おき（これが既に存在する他のソフトウェアに相当する）、利用者側では、前者の有償の暗号化ソフトウエアを購入し、これを復号して得られたソフトウェアを用いて、後者の配布されたソフトウェアを実行する（例えば後者のソフトウェアが前者のソフトウェアを呼び出すことにより全機能が実行可能となる）。

【００３３】このようにすれば、利用者は、機能等の限定された無償配布のソフトウェアを実際に試用した上で、気にいった場合だけ有料の追加機能を購入することができるなど、種々の利点がえられる。

【００３４】なお、ソフトウエアの一部分（機能等の限定されたもの）を無償で配布しておき（これが既に存在する他のソフトウェアに相当する）、該ソフトウエアの他の部分を暗号化して有償で提供し（これを復号したものが、復号により得られたソフトウェアに相当する）、利用者側では購入した暗号化ソフトウエアを復号し、これを上記ソフトウエアの一部分に取り込んで実行するような形態も可能である。

【００３５】本発明（請求項６）は、ソフトウエア提供者が指定されたソフトウェアを暗号化して利用者に提供するソフトウエア流通システムにおいて、ソフトウェア料金の決済に関わる識別情報との対応付けが保証された共有鍵を記憶する、ソフトウェア提供者及び利用者側の双方に設けられた共有鍵記憶手段と、指定するソフトウエアの提供の要求をソフトウエア提供者に送る、利用者側に設けられた要求送信手段と、指定されたソフトウエアを前記共有鍵と関連付けて暗号化する、ソフトウエア提供者側に設けられたソフトウエア暗号化手段と、この暗号化されたソフトウエアを前記利用者に送信する、ソフトウエア提供者側に設けられた暗号化ソフトウエア送信手段と、受信した暗号化ソフトウエアを前記共有鍵と関連付けて復号する、利用者側に設けられたソフトウエア復号手段とを具備したことを特徴とする。

【００３６】好ましくは、前記ソフトウエア提供者側に、受信したソフトウエアの提供の要求が正当であるか否かを前記共有鍵と関連付けて検査する要求検査手段と、前記検査の結果、正当であると判断された場合にのみ、前記ソフトウエア暗号化手段と前記暗号化ソフトウエア送信手段に夫々暗号化と送信の実行を指示するソフトウエア送信指示手段とをさらに設けたことを特徴とする。

【００３７】正当性の検査は、例えば、ソフトウエア提供者と利用者で同一のハッシュ関数を持ち、共有鍵を入力とするハッシュ関数の出力を利用者からソフトウエア提供者に送り、ソフトウエア提供者側で、該共有鍵を入力とするハッシュ関数の出力を求め、両出力を比較することにより実現できる。これによって、不正な要求を把握することができる。

【００３８】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。ソフトウエア流通のメカニズムは、暗号技術が基本となっており、それをいかに利用して安全なシステムを構築するかがポイントとなる。データ暗号化のアルゴリズム自体は様々あり公知の方式を使えばよいので、ここではその説明は省略する。なお、データ暗号化のアルゴリズムの詳細については、文献（「暗号と情報セキュリティ」昭晃堂）などに詳しく記述されている。

【００３９】暗号化に先立って暗号化に必要な秘密の鍵を生成し、この秘密の鍵をあらかじめ通信相手と自分とが持っていれば良いが、一般にソフトウエアの流通を考えた場合にはその仮定はできないので、最初に鍵を交換しなければならない。このような目的としては公開鍵暗号方式を用いることができる。公開鍵暗号方式では例えばソフトウエアを販売する店舗が「公開鍵」および「秘密鍵」と呼ばれる２つの鍵を持っている。転送したいデータは、送信側にて公開鍵で暗号化し、受信側にて秘密鍵で復号する。公開鍵は文字通り公開される鍵なので、誰に見られても良い。この公開鍵を使って顧客に「秘密の鍵」（秘密鍵とは別のものである）を暗号化して送ってもらう。秘密鍵を持っている店舗はこれを復号し、「秘密の鍵」を得る。この方式では、万一通信データが盗み読まれても、秘密鍵を知らない者はデータを復号することができない。公開鍵暗号方式としては、米国ＲＳＡ社のＲＳＡ方式が良く知られている。またこれら技術を組合わせることにより、店舗にさえクレジット番号を知られずにクレジット会社に転送できる電子決済用のプロトコルＳＴＴ(Secure Transaction Technology)やＳＥＰＰ(Secure Electronic Payment Protocol)なども使われ始めた。これらのプロトコルは、顧客、店舗、決済会社の３者間のセキュリティを考慮したものであるのに対し、本発明は、特に顧客と店舗との間のやりとりを改善するものである。本実施形態においては特に後者に関する説明を中心に行うが、本発明はこられの技術を組合わせて３者間のやりとりなど他の形態にも応用することもできる。

【００４０】図１に本発明を適用したソフトウエア流通システムの典型的な実施形態を示す。図１で左側はソフトウエアを販売しようとする店舗側、右側は購入しようとする顧客側、その間は両者を結ぶネットワークである。ここで言うソフトウエアとは、計算機プログラム、データベース、情報検索サービスによって得られた結果、書籍、音楽、映画、テレビ放送、対戦型ゲームや電話あるいは対話型テレビなどでインタラクティブに交換される情報など、物流を伴わずに電子的に送信することが可能なもの全てを含むものとする。

【００４１】まず、課金は、そのソフトウエアを入手しようとする人が誰であるかを特定し、その人の銀行口座、クレジットカードの口座、電子マネーなどを用いて決済することである。その際、不正に料金をごまかした

り、不正な手段でソフトウエアを入手したり、他人の口座を不正に利用してソフトウエアを入手したり、他人の意思に反してその人に購入させたり、自分が購入したにもかかわらず後日になって自分は買っていないと主張したり、購入してもいない顧客に、店が勝手に買ったことにしたり、計算機ネットワークに流れるデータを盗み読んで他人の口座番号を入手したり、といったさまざまな不正が防止できるシステムを構築しなければならない。

【００４２】また、違法コピーの防止も重要である。どんなに完全な課金メカニズムがあっても、ソフトウエアは一般に容易にコピー（複製）を作成することができるので、購入したソフトウエアを無料で他人に配ったり、または安い値段で違法に転売することができてしまう。特に計算機ネットワークの発達した今日では、暗号電子メールや掲示板といった情報交換の手段を用いれば、こういった違法行為を他人の知り得ない水面下で行うことが可能になっており、これは重要な課題となっている。

【００４３】図１に示すように、店舗はあらかじめ公開鍵暗号方式による店舗秘密鍵１０１と店舗公開鍵１０２を持っている。店舗秘密鍵１０１は店舗秘密鍵格納部５０に保存されており、他からはその内容を参照できない。店舗公開鍵１０２は公開されていて、誰でもネットワークをするなどの手段で入手することができる。入手のメカニズムは鍵配布局などの従来方式が知られており、ここでは説明を省略する。

【００４４】本実施形態においては、まず顧客がクレジットカード等の支払能力を示す信用を持っていることを示すためのユーザ登録、次に実際に注文を行う注文部分、購入したソフトウエアを利用する利用部分の３段階に分かれる。一旦ユーザ登録した顧客は次回からユーザ登録なしに注文を行う仕組みとして示す。なお、本実施形態はユーザ登録と注文を同時に行うものとし両者を合わせて注文部分とするような形式に変更することは容易に可能であるため、より一般化した方式をもって以下説明している。

【００４５】以下、３段階夫々について順次説明する。顧客がソフトウエアを購入する際には、まず店舗との安全な通信を確保するために共有鍵生成部２によって共有鍵１０３を生成する。これは他からは推測できない乱数を生成するものである。従来技術ではこの共有鍵１０３は注文および購入のときにのみ使われ使用後は保存せずに捨てられていたが、本実施形態においては、共有鍵暗号化部（Ｂ）２０で暗号化され、得られた暗号化共有鍵２０２は、共有鍵格納部２２に保存される。

【００４６】共有鍵暗号化部（Ｂ）２０では、暗号化の際に、付加情報検出部８の得た付加情報２０３を鍵として利用する。付加情報２０３とは具体例として、顧客の持つ計算機に固有の番号（ｈｏｓｔＩＤ）や、利用しているＯＳの商品番号や、そのユーザしか知り得ないパスワードや、ユーザの持っているＩＣカードに入っているデータまたはＩＣカードに何らかのデータを与えて出力される結果データ、計算機に内蔵された時計の時刻などである。

【００４７】共有鍵暗号化部（Ｂ）２０が、共有鍵１０３の暗号化に付加情報２０３を使うことにより、共有鍵格納部２２の盗聴などによる安全性の低下を防止する。また、どの付加情報を選択するかによって、例えば、同一のマシンであればずっとソフトウエアを使い続けられるとか、同一のマシンであっても、新しいＯＳになった時には再度お金を払わなければソフトウエアが利用できなくなるとか、ある時刻（日付）になったら再度お金を払う必要があるとか、夜間の使用は無料だが、昼間の使用は制限されるなどといった、さまざまな形態での課金方法が可能になる。また、付加情報として、ユーザがその時点で入力するパスワードを使うことも可能であり、その場合、ソフトウエアの利用を、特定のパスワードを知っている者に限るという応用も、付加情報検出部８の設定を変更するだけで、容易に可能である。

【００４８】なお、共有鍵暗号化部（Ｂ）および２０付加情報検出部８を設けないようにすることは自由である。この場合、共有鍵生成部２で生成された共有鍵１０３は、そのまま共有鍵格納部２２に格納される。

【００４９】さて、上記のようにして生成された共有鍵１０３は共有鍵暗号化部（Ａ）１２によって暗号化される。暗号化の際には店舗公開鍵１０２を利用する。共有鍵暗号化部（Ａ）１２は、生成された暗号化共有鍵１０４を共有鍵送信部１４に送り、共有鍵送信部１４はこれをネットワークを介して店舗側に送信する。店舗側の共有鍵復号部（Ｂ）５２は、受信した暗号化共有鍵１０４を店舗秘密鍵１０１を用いて復号し、共有鍵１０３を得る。

【００５０】また、ＩＤ生成部４は、店舗がこの顧客を他の顧客と区別するためのＩＤ２０１を生成する。これは基本的には任意の乱数で良いが、他の顧客の作成したＩＤと重複すると後の処理が複雑になるため、なるべく重複しない形で作成する。例えば、作成した時刻と、顧客の持つ計算機のＩＤを組合わせるなどする。ＩＤ２０１は登録リクエスト暗号化部１６に送られると同時にＩＤ格納部２４に保存される。ＩＤの格納は共有鍵の格納の場合と全く同様の手順で暗号化し、保存することも可能であるが、ここでは暗号化しないものとして説明する。

【００５１】一方、顧客は、ユーザ情報入力部６によってユーザ情報の入力を行う。ユーザ情報とは、例えば、与信に用いる情報、住所、氏名、年齢、（登録と同時に注文する場合における）そのユーザが購入したいソフトウエアの名前、などである。

【００５２】与信に用いる情報とは、その顧客が確かに決済（支払）をする能力を持ち、しかも注文に対して責任が負える人であるということを示す情報であり、例え

は、クレジットカード番号やその有効期限、暗証番号などが相当する。また、決済の手段によっては、銀行の口座番号、特定の企業等から発行された決済に関わる会員番号等（例えばパソコン通信のユーザＩＤ）などである場合もある。本実施形態においては、説明を簡略化するために、これらを代表してクレジット・カード番号と呼ぶことがある。

【００５３】ここで入力されたユーザ情報１０５は、登録リクエスト暗号化部１６に送られる。登録リクエスト暗号化部１６は、受信したＩＤ２０１とユーザ情報１０５を、共有鍵１０３を用いて暗号化し、出力である暗号化登録リクエスト２０４は登録リクエスト送信部１８によってネットワークを介して店舗側の登録リクエスト復号部５４に送信される。

【００５４】登録リクエスト復号部５４は、受信した暗号化登録リクエスト２０４を共有鍵１０３で復号し、ユーザ情報１０５およびＩＤ２０１を得る。このＩＤが過去に他の顧客用に使われたＩＤと重複していないことを確認し、正式なＩＤとなる。万一、ＩＤが重複していれば、以上述べた手順を最初からやり直す。確認およびやり直しの方法は公知かつ容易であるため説明を省略する。

【００５５】そして、登録リクエスト復号部５４は、顧客情報１０８を顧客情報確認部５６に送る。ここで顧客情報とは受信し復号したユーザ情報１０５のうち、決算に関する部分である。例えばクレジットカード番号や氏名がこれである。また、顧客情報確認部５６は、例えばクレジットカード等に関する顧客信用調査機関（のシステム）に問い合わせをして、顧客の信用を確認する。

【００５６】ところで、ここまでの説明は、顧客から店舗への通信は、ＩＤ２０１とユーザ情報１０５を共有鍵１０３で暗号化するという方式で行ったが、別の形態もあり得る。図２は、ＩＤ２０１、ユーザ情報１０５および共有鍵１０３を全て店舗公開鍵１０２で暗号化して送る例において、図１と相違する部分を示したものである。この場合、共有鍵生成部２で生成された共有鍵１０３、ＩＤ生成部４で生成されたＩＤ２０１、およびユーザ情報入力部６´で得られたユーザ情報１０５はいずれも登録リクエスト暗号化部１６´に送られ、登録リクエスト暗号化部１６´はこれらを店舗公開鍵１０２で暗号化し、得られた暗号化登録リクエスト２０４´を登録リクエスト送信部１８´に伝える。登録リクエスト送信部１８´が送信した暗号化登録リクエスト２０４´は、登録リクエスト復号部５４´が受信し、店舗秘密鍵１０１で復号し、ユーザ情報１０５、ＩＤ２０１および共有鍵１０３を得る。これ以外の部分は図１においてここまでに説明した構成およびこれから説明する構成と同様である。

【００５７】さて、ユーザ情報格納部５８は、顧客情報確認部５６の確認した信用情報１１０に基き、この顧客が、今後ソフトウエアを販売しても良いユーザであれば、登録リクエスト復号部５４から得たユーザ情報１０５、ＩＤ２０１および共有鍵１０３を対応付けて格納する。

【００５８】ユーザ情報格納部５８に格納されるデータ構成の一例を図３に示す。図３では、各顧客の情報が登録順に整理されている。もちろん、登録順にする必然性はないが、例えばＩＤ生成部４の生成するＩＤに重複を避けるための時刻情報を付加するとすれば、ＩＤの重複検査は比較的最近登録された顧客のＩＤだけをチェックすれば良いので容易になる。

【００５９】図３のように、各顧客について、ＩＤ、共有鍵、クレジット・カード番号、個人情報が記録されている。ＩＤはその顧客に固有の番号で、その顧客の共有鍵やクレジット・カード番号などを取り出す際に使われる。

【００６０】共有鍵の機能については他で説明する通りである。クレジット・カード番号は、その人の決済用の番号である。クレジット・カード番号にはクレジット・カードの有効期限などが含まれる場合もあり、銀行口座からの決済であれば銀行口座の番号またはそれを指定するためのユーザ固有の番号などが入る。

【００６１】また、クレジット・カード番号は、その店舗が顧客名を指定するためにクレジット・カード会社に送るデータであるため、必ずしもカード番号そのものが書かれている必要はない。例えば、カード会社がその店舗に知らせる目的で発行する顧客番号を格納しておくことも可能である。そのような方法であれば、店舗が顧客のカード番号等を保管する必要はないので、ユーザ情報格納部５８の盗難などに対する安全性が高まる。これについては電子決済プロトコルなどで知られている従来のやり方で改良が可能なので、ここでは説明を省略する。

【００６２】個人情報は、その顧客に関する付加的な情報であり、決済上は特に意味を持たなくても良い。ただし、そのユーザの信用調査などの目的でここに記録された個人情報を参考として使うことはあり得る。

【００６３】ここで、図３において登録順が４の顧客は、ＩＤ以外のフィールド情報が消えている。これは、何らかの理由でこの顧客への販売が停止されたことを意味している。販売が停止されてもＩＤを残している理由は、万一、同一のＩＤの顧客が新たに登録された場合、元の顧客からの注文が出たときの処理が複雑になるからである。ただし、現実には共有鍵が異るので不正に注文することはできないので、一定期間後に消去しても良い。

【００６４】また、図３において、登録順が５の顧客はクレジット・カード番号のフィールドだけが消えている。これは、その顧客のクレジット・カードが無効になったことを意味している。しかし、共有鍵は有効であるため、店舗はこのユーザの正当性は依然として認めてい

ることを意味している。クレジット・カード番号を新たに登録するなどにより、再度その顧客は注文ができるようになる。以後、このユーザ情報格納部５８に格納されたユーザ情報１０５とＩＤ２０１を元に、顧客へのソフトウエア販売を行う。

【００６５】なお、図３において、説明を簡単にするために各データは暗号化せずに記録されているものとして記述したが、実際のシステム では盗難に対するセキュリティなどの理由で、暗号化して保存するのが好ましい。例えば、共有鍵を保存するかわりに暗号化共有鍵を保存してもよい。これについては従来技術で容易に実現できるので、ここでの詳しい説明は省略する。

【００６６】以上、ユーザ登録の部分を詳細に説明した。次に、実際に注文を行う注文部分について説明する。顧客はソフトウエア指定部１０によって購入するソフトウエアの名前などの商品指定データ１０６を入力する。商品指定データ１０６はハッシュ部２８とリクエスト送信部２６に送られる。ＩＤ格納部２４から取り出されたＩＤ２０１もハッシュ部２８とリクエスト送信部２６に送られる。一方、共有鍵復号部（Ａ）３０は、共有鍵格納部２２から取り出した暗号化共有鍵２０２を、付加情報検出部８によって検出された付加情報２０３を用いて復号し、共有鍵１０３を得る。

【００６７】ハッシュ部２８は、商品指定データ１０６とＩＤ２０１を、共有鍵１０３を用いてハッシュし、得られたハッシュ値２０５をリクエスト送信部２６へ送る。ここで、ハッシュするとは、入力データに対して特定の関数（この関数は店舗側と同一のものが共有されている）を適用してある値（ハッシュ値）を求めることであるが、この関数は出力から元の入力が推測できない性質を持ったものであり、一般にハッシュ関数と呼ばれている。ハッシュ関数の作り方については従来技術を使用すれば良く、ここでは説明を省略する。

【００６８】リクエスト送信部２６は、商品指定データ１０６と、ＩＤ２０１と、ハッシュ値２０５を店舗側に送信する。店舗側のリクエスト受信部６０は、これらデータを受信し、該当ＩＤを持つ顧客の共有鍵１０３をユーザ情報格納部５８より読み出す。該当ＩＤが存在しなければエラーとし、注文を受け付けない。

【００６９】ハッシュ部６２は、商品指定データ１０６とＩＤ２０１を、共有鍵１０３を用いてハッシュし、サーバ・ハッシュ値２０５´を得、リクエスト検査部６４に送る。リクエスト検査部６４はこのサーバ・ハッシュ値２０５´を、リクエスト受信部６０から受取ったハッシュ値２０５と比較する。ハッシュ部６２の機能は顧客の持つハッシュ部２８と全く同一であるから、ハッシュ値２０５とサーバ・ハッシュ値２０５´は同一のはずである。万一、これが一致しない場合には、正しい共有鍵を持たないユーザからの注文であるか、または他人の注文した商品の名前が書換えられた、などの不当な注文であることを意味する。なお、後に説明する通り、仮にこのチェックをせずにソフトウエアを販売したとしても、共有鍵を持たない者は利用することができないのであるが、それでもやはりこのチェックは必要である。なぜなら、他人の名前を語った不当な注文をいやがらせ等で行う者もあるかもしれないからである。

【００７０】リクエスト検査部６４は、ハッシュ値２０５とサーバ・ハッシュ値２０５´とが一致した場合、その旨をソフトウエア送信指示部６６に伝える。この時点で、顧客からの購入要求（注文）があったことが正当に証明され、決済を行うことができる。具体的な決済の方法については、従来の電子決済などで知られた方法を用いればよく、ここでは説明を省略する。

【００７１】なお、厳密には、ここで説明したリクエスト送信方法では不十分な場合がある。例えば、通信を盗聴し、全く同じリクエストを店舗に繰り返し送信することにより、共通鍵を持たない者が不正な注文をすることができる。これは一般にリプレイ・アタックと呼ばれる不正であり、これを回避するためにリクエストに注文時刻情報や相手（店舗）の発行する通し番号を付けるなどの方法が知られている。これら暗号技術の詳細は従来技術を組み合わせることとし、本実施形態では説明を省略する。

【００７２】ソフトウエア送信指示部６６は、共有鍵１０３をソフトウエア暗号化部７０に送ると共に、暗号化ソフトウエア送信部７２に送信を指示する。ソフトウエア暗号化部７０は、ソフトウエア格納部６８より読み出した該当ソフトウエア１１３を共有鍵１０３で暗号化し、得られた暗号化されたソフトウエア１１４を顧客側に送信する。なお、ソフトウエアの暗号化は、そのままの形で実行したり参照したりすることが不可能であるような形にすることが目的であり、必ずしも一般的なデータの暗号化を行う必要はない。例えば、パスワード入力をしないと実行できない仕組みを持った計算機プログラム は暗号化されたソフトウエアの一種と考えることもできる。本実施の形態においては、暗号化されたソフトウエアとは特に断らない限りこの意味の広い解釈をするものとする。送信された暗号化されたソフトウエア１１４は顧客側の暗号化ソフトウエア格納部３２に保存される。

【００７３】以上、注文の部分を詳細に説明した。次に、実際にソフトウエアを利用する利用部分について説明する。まず、顧客側の共有鍵復号部（Ａ）３０は、共有鍵格納部２２から取り出した暗号化共有鍵２０２を、付加情報検出部８によって検出された付加情報２０３を用いて復号し、共有鍵１０３を得る。ここまでは注文の際の共有鍵の取り出しのメカニズム と同一である。ソフトウエア復号部３４は、暗号化ソフトウエア格納部３２より取り出した暗号化されたソフトウエア１１４を得られた共有鍵１０３で復号し、ソフトウエア１１３を得

る。

【００７４】以上の方法によって、実際にクレジットカード番号等を伝えた正規のユーザのみにソフトウエアを販売することができる。また、共有鍵１０３を付加情報２０３によって暗号化保存するという形態を取っているため、単純に共有鍵復号部（Ａ）３０、共有鍵格納部２２、暗号化ソフトウエア格納部３２の全てをコピーしても、ソフトウエアを違法コピーすることはできない。また、ソフトウエアの動作メカニズム を解析して違法コピーを作り出すことは難しく、手間をかけてまで違法コピーする価値はなくなる。また、従来技術においては、違法コピーを配布することが本人にとって損失がなかったため、防止する手段に乏しかったが、本実施形態においては、暗号化の基となる共有鍵１０３は、ソフトウエアの実行に対する鍵であ ると同時に、ソフトウエア購入の鍵でもあ るため、共有鍵をセットにした違法コピーを行うと、自分自身のクレジットカード番号によって、他人が新たなソフトウエアを購入してしまい、損害が自分自身に降りかかる危険があ るという特徴を持ち、違法行為防止の効果があ る。

【００７５】また、本実施形態のソフトウエア流通システム においては、一旦ユーザ登録を済ませたユーザは、その計算機を持っているだけで、クレジットカード番号等のデータ入力をすることなくソフトウエアの購入ができるという簡便な方法を採用したにもかかわらず、安全に課金を行うことができる。また、本実施形態のソフトウエア流通システム では、顧客が固有の公開鍵を持っている必要がない。つまり、クレジット・カード番号を持っているといった比較的単純な条件を元に販売をすることが可能であ る。

【００７６】さらに本実施形態の応用として、ソフトウエアの全体をこの方式で販売するのではなく、一部だけにこの方式を使うことができる。例えば、図４はこの部分を改良した一方式を示したものであ る。図４のコア・ソフト部３５は、図１のソフトウェア復号部３４に相当するプログラム であ る。

【００７７】コア・ソフト部３５は、計算機プログラムの主たる部分であ り、このままでは完全には動作しない。これに暗号化ソフトウェアを追加することによって機能を追加することができる。つまり、暗号化ソフトウエアを復号する権 限のない者が実行しても、全ての機能が動作するわけではない。

【００７８】コア・ソフト部３５が実行されるとまず、ソフトウエア復号部３５１は、暗号化ソフトウエア格納部３５２に、そのコア・ソフト部３５に対応する暗号化されたソフトウエアが存在するかどうか調べる。存在した場合には、暗号化されたソフトウェア１１４を読み出し、共有鍵１０３で復号し、結果として得られた復号ソフト３０１を復号ソフトローディング部３５２に格納する。もし、共有鍵１０３を得られない場合は、復号ソフトローディング部３５２には正しいデータが格納されない。

【００７９】コア・ソフト部３５は、ここに配置された復号ソフト３０１が正しいデータであ ることを確認する。確認の方法は、例えばここに格納された復号ソフト３０１が、コア・ソフトによってあ らかじめ予定されたデータに等しい（正しく復号されている）ことをチェックするという方法と、ここに格納された復号ソフト３０１そのものをプログラム として実行するという方法が代表的であ る。

【００８０】このような構成にすることによる様々な利点を以下に述べる。まず、コア・ソフト部をあ るソフトウェアの機能限定版とし、該ソフトウェアの有料部分だけを暗号化ソフトウエアとして販売することができる。例えば、コア・ソフトは、印刷機能と通信機能が制限されたワードプロセッサであ り、印刷機能と通信機能はそれぞれ有料のソフトウェアとして販売される。この方法を用いれば、例えばソフトウエアを購入の都度店舗が送信するのではなく、ＣＤ－ＲＯＭや電子掲示板のような誰でも入手し参照することが可能な媒体でコア・ソフトを無料配布しておき、好評ならば有料部分を購入してもらうということができる。

【００８１】従来の通信販売の場合、品物が確かめられない制約から、クーリング・オフという制度があ るが、形を持たないソフトウエアの場合、一旦購入した物を返品することが不可能であ る。したがって、図４で示したコア・ソフトをまずお試し版として顧客に利用してもらうことにより、クーリング・オフのできないことによる顧客の不利益を防ぐことができる。実際に試用した上で、気にいった場合だけ有料の追加機能を購入することができる。また、この追加機能は１つだけでなく複数設定することもできるので、「有料」と「無料」の２種類だけでなく、必要な部分だけを適正な価格で買うことができる（不要機能まで抱き合わせ販売されてしまうという不公正流通が防げる）。

【００８２】次に、暗号化や復号に必要なデータ量が削減できる。一般に、暗号化や復号の計算はデータ量に比例した時間がかかるため、非常に大きなサイズのソフトウェアをその都度暗号化して販売すると、購入（ダウンロード）に時間がかかったり、実行（復号）の際に時間がかかったりするので、暗号化の必要な部分はなるべく小さくする必要があ る。

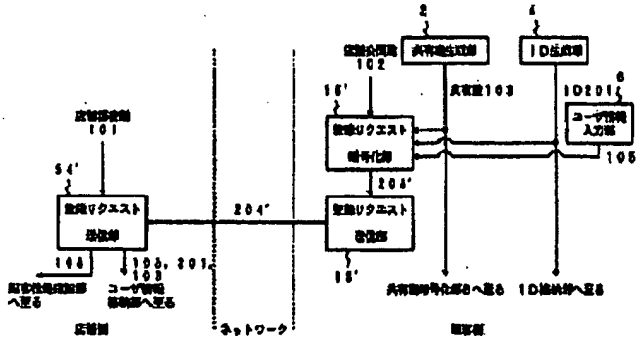
【００８３】有料の追加機能部分がデータ量としては非常に小さい場合であ れば、暗号化する部分としない部分とに分割するだけでこの要求が満たされるが、有料の追加機能部分が大きかったり、ソフトウェア全体が有料であ ったりする場合には、図４で示した仕組みを使うことにより、ソフトウェアそのものはコア・ソフトに格納されているが、暗号化ソフトウェアを復号しない限り、有料部分は機能しないようにコア・ソフトを予め作成して

おくことができる。
【００８４】また、データ量が削減できるということは、通信回線が細くても良いということを意味する。つまり、有料機能を買うための店舗と顧客との通信回線が遅い場合、一般にはダウンロードに時間を要してしまうが、コア・ソフト部分だけはＣＤ－ＲＯＭで配布しておいたり、他の高速ネットワークを通じて入手したりしておけば、あ とはごく小さな暗号化ソフトウェアだけを入手すれば良く、購入に時間がかからなくなる。
【００８５】さらに、違法コピーを防ぐ別の方法としても用いることができる。例えば、販売するソフトウェアが書籍である場合、最終的にはメモリ上で計算機等で読める形式の文字列データに変換されてしまうため、そのデータをメモリ上から盗み読むことは比較的簡単にできてしまう。しかし、コア・ソフトは「書籍を読むソフト」としておき、有料の追加機能である個々のソフト（書籍）を読み込んで、その内容を画面に表示するという仕組みにしておくことができる。この場合、コア・ソフトが必要なデータ（暗号化されたデータ）を随時復号して表示する仕組みにすれば、書籍のデータ（文字）全部をまとめて読み出すというのは非常に困難になる。
【００８６】また、復号されたソフトウェアは、コア・ソフトの実行される際のメモリ上に存在するだけになるので、コア・ソフトが暗号化ソフトウェアを利用する方法手順を煩雑にすることによって、販売されたソフトウェアの暗号を解く手間が非常に大きくなり、安全性が高まる。一般に、ネットワークで販売されるソフトウェアは、バージョンアップが比較的頻繁であったり、一時的にしか価値のない情報（例えば天気予報）のようなものである場合が多く、ソフトウェアの違法コピー作成に知恵を絞るよりも、正しくお金を払ってソフトウェアを購入した方がはるかにコストが安くなるため、違法行為を行う意味がなくなり、ソフトウェアの公正な流通が促進される。
【００８７】なお、本実施の形態の説明においては、ソフトウェアを有料で販売することを前提として記述したが、必ずしも有料である必要はない。例えば、特定国家への輸出が禁止されているソフトウェアを配布する際に、ユーザ情報を元に特定の顧客にしかソフトウェアを配布しない、という使い方も、本実施形態の技術的範囲にて実現できることは明らかである。
【００８８】また、図４におけるコア・ソフト部に、本実施形態で説明した注文部分に相当する機能を追加すれば、ソフトウェアの利用のたびに利用料金を課金する仕組みも、単純な改造で実現できることが明らかである。
【００８９】なお、本実施形態で説明したソフトウェア流通システムは、その実行手順を計算機上のプログラムなどで置き換えることにより、ソフトウェアで実現することもできる。
【００９０】以下に、本実施形態のソフトウェア流通システムにより得られる主な効果を挙げる。購入の際にクレジット・カード番号を入力するような手間をかけない簡便な方法でソフトウェアを購入することができると共に、安全に課金を行うことができる。また、何に対して課金をするかといった細かな指定が可能であることと相まって、各ソフトウェアの価値に応じた適正な価格での販売が促進される。
【００９１】消費者は、汎用用途のクレジット・カードなどを使って、自発的に自分の希望する店舗での購入を可能とする共有鍵を作成することができ、店舗が発行する会員番号などを記憶しなくても、日頃クレジット・カードを保管したままでソフトウェアの購入ができるので安全である。しかも、万一共有鍵が盗まれても、用途が限定されているため、被害は少ない。この共有鍵は、従来のクレジットカードよりも汎用性を下げているため万一の場合の被害が少なく、また、プリペイド・カードのように予めお金を払う必要もないと同時に、自分の意思で必要に応じて作ったり捨てたりすることができることが特徴である。
【００９２】また、共有鍵はソフトウェアの実行に対する鍵であると同時に、ソフトウェア購入の鍵でもあり、ソフトウェアの違法コピーを行うことが困難でリスクの高いものになるため、違法行為を行う価値がなくなり、著作権者の権利が守りやすくなる。
【００９３】本発明の目的の一つは、煩雑な手順なしでソフトウェアのインストールが行えるようにすることであるが、容易にインストールする仕組みを提供するとことによって、顧客個人の持つプログラム・ファイル等のデータが書き換えやすくなるため、例えば悪意の者が通信を盗み取って偽の店舗をつくり、プログラムを顧客に提供するといったセキュリティー・ホールになりかねない。本発明の仕組みを用いれば、ソフトウェアは店舗と顧客の両者しか知り得ない共有鍵で暗号化されて提供されるため、万一悪意の者が不正にソフトウェアを提供する課程に成功したとしても、その者の意図したデータを作り上げることはできないので、顧客側からそれを容易に検出することができ、また検出されずとも「ウイルス」と呼ばれるような特定の悪い動作をする計算機プログラムがインストールされるといったことはなくなり、ソフトウェア流通の安全性が高まる。本実施形態は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。
【００９４】
【発明の効果】本発明によれば、ソフトウェア提供者が利用者に暗号化ソフトウェアを提供する際に用いる共有鍵が、ソフトウェア料金の決済に関わる識別情報と結び付けられているので、該共有鍵を共有する利用者は、注文の都度、識別情報を入力する必要がなく、簡易な操作でネットワークを介したソフトウェアの購入ができ、ソフトウェア提供者は、ソフトウェア流通を公正な価格で

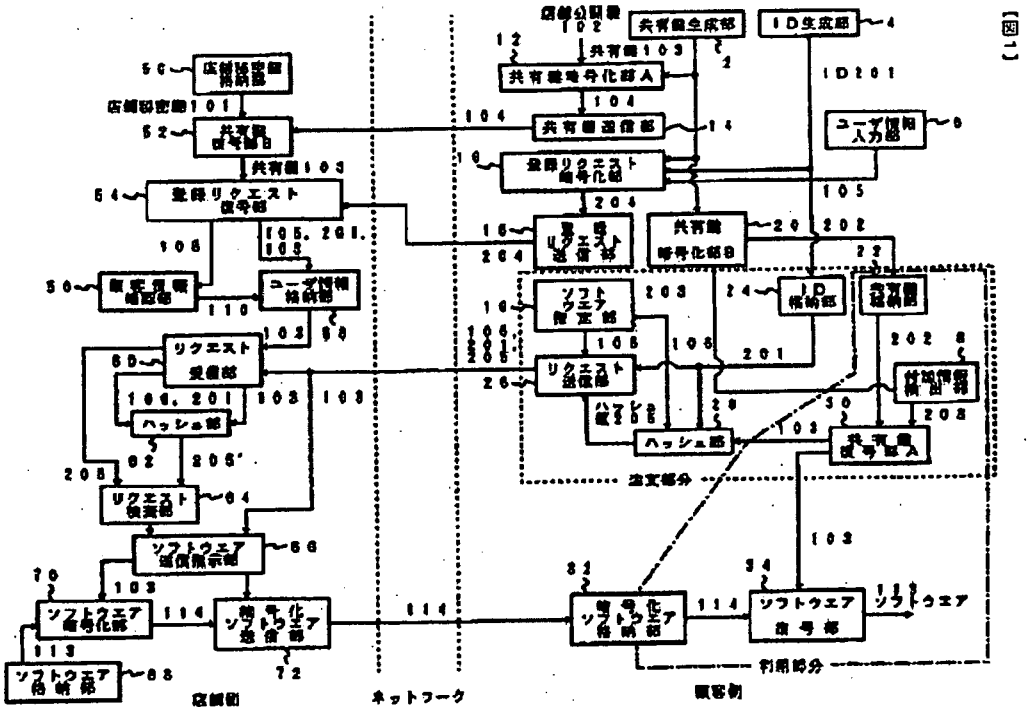
安全に行うことができ、また、ソフトウエアの違法コピーが利用者にとって不利益となるので、違法コピーを困難とすることができる。

【図面の簡単な説明】
【図１】本発明の実施形態に係るソフトウエア流通システム の構成例を示す図
【図２】ＩＤとユーザ情報を公開鍵で暗号化する場合の構成例を示す図
【図３】ユーザ情報格納部に格納されている情報の一例を示す図
【図４】コア・ソフトを使った応用例を示す図
【図５】従来のソフトウエア流通システム の構成図の例
【符号の説明】
２…共有鍵生成部
４…ＩＤ生成部
６…ユーザ情報入力部
８…付加情報検出部
１０…ソフトウエア指定部
１２…共有鍵暗号化部（Ａ）
１４…共有鍵送信部
１６，１６´…登録リクエスト暗号化部
１８，１８´…登録リクエスト送信部
２０…共有鍵暗号化部（Ｂ）
２２…共有鍵格納部
２４…ＩＤ格納部
２６…リクエスト送信部
２８…ハッシュ部
３０…共有鍵復号部（Ａ）
３２…暗号化ソフトウエア格納部
３４…ソフトウエア復号部
３５…コア・ソフト部
３５１…ソフトウエア復号部
３５２…復号ソフトローディング部
５０…店舗秘密鍵格納部
５２…共有鍵復号部（Ｂ）
５４，５４´…登録リクエスト復号部
５６…顧客情報確認部
５８…ユーザ情報格納部
６０…リクエスト受信部
６２…ハッシュ部
６４…リクエスト検査部
６６…ソフトウエア送信指示部
６８…ソフトウエア格納部
７０…ソフトウエア暗号化部
７２…暗号化ソフトウエア送信部

【図２】



【図１】

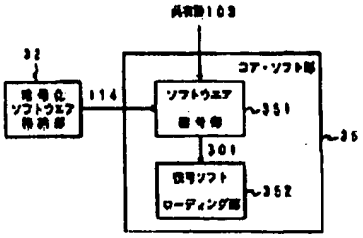


【図3】

ユーザ情報105

登録No.	ID$_{111}$	共有鍵101	クレジットカード番号	個人情報
1	3625603	6827641	22-52-6643	山田太郎 〒100 港区…
2	2163430	3287621	21-66-3229	山田花子 〒144 蒲田区…
3	3353162	3562387	44-22-2152	鈴木一郎 〒220 横浜…
4	4521187	-	-	-
5	5613215	5003214	-	佐藤二郎 〒220 横浜…
6	4597514	2392362	21-62-3315	高橋一郎 〒146 大田区…
7	4457361	6473219	33-25-4111	渡辺 誠 〒220 横浜…
⋮				

【図4】



【図5】